

Department of the Air Force, DoD

§ 806b.7

command disciplinary action, and consult the servicing Staff Judge Advocate. In combatant commands, process component unique system complaints through the respective component chain of command.

(b) For Privacy Act complaints filed in a U.S. District Court against the Air Force, an Air Force activity, or any Air Force employee, Air Force Legal Services Agency, General Litigation Division (JACL) will provide Air Force Chief Information Officer/P a litigation summary to include: The case number, requester name, the nature of the case (denial of access, refusal to amend, incorrect records, or specify the particular violation of the Privacy Act), date complaint filed, court, defendants, and any appropriate remarks, as well as updates during the litigation process. When the court renders a formal opinion or judgment, Air Force Legal Services Agency, General Litigation Division (JACL) sends Air Force Chief Information Officer/P a copy of the judgment and opinion.

§ 806b.5 Personal notes.

The Privacy Act does not apply to personal notes on individuals used as memory aids. Personal notes may become Privacy Act records if they are retrieved by name or other personal identifier and at least one of the following three conditions apply: Keeping or destroying the records is not at the sole discretion of the author; the notes are required by oral or written directive, regulation, or command policy; or they are shown to other agency personnel.

§ 806b.6 Systems of records operated by a contractor.

Contractors who are required to operate or maintain a Privacy Act system of records by contract must follow this part for collecting, safeguarding, maintaining, using, accessing, amending and disseminating personal information. The record system affected is considered to be maintained by the Air Force and is subject to this part. Systems managers for offices who have contractors operating or maintaining such record systems must ensure the contract contains the proper Privacy Act clauses, and identify the record

system number, as required by the Defense Acquisition Regulation and this part.

(a) Contracts for systems of records operated or maintained by a contractor will be reviewed annually by the appropriate Major Command Privacy Officer to ensure compliance with this part.

(b) Disclosure of personal records to a contractor for use in the performance of an Air Force contract is considered a disclosure within the agency under exception (b)(1) of the Privacy Act (see § 806b.47(a)).

§ 806b.7 Responsibilities.

(a) The Air Force Chief Information Officer is the senior Air Force Privacy Official with overall responsibility for the Air Force Privacy Act Program.

(b) The Office of the General Counsel to the Secretary of the Air Force, Fiscal and Administrative Law Division (GCA) makes final decisions on appeals.

(c) The General Litigation Division, Air Force Legal Services Agency (JACL), receives Privacy Act appeals and provides recommendations to the appellate authority. Service unique appeals, from combatant commands, should go through the respective chain of command.

(d) The Plans and Policy Directorate, Office of the Chief Information Officer manages the program through the Air Force Privacy Act Officer who:

(1) Administers procedures outlined in this part.

(2) Reviews publications and forms for compliance with this part.

(3) Reviews and approves proposed new, altered, and amended systems of records; and submits system notices and required reports to the Defense Privacy Office.

(4) Serves as the Air Force member on the Defense Privacy Board and the Defense Data Integrity Board.

(5) Provides guidance and assistance to Major Commands, field operating agencies, direct reporting units and combatant commands for which AF is executive agent in their implementation and execution of the Air Force Privacy Program. Ensures availability of training and training tools for a variety of audiences.

§ 806b.8

(6) Provides advice and support to those commands to ensure that information requirements developed to collect or maintain personal data conform to Privacy Act standards; and that appropriate procedures and safeguards are developed, implemented, and maintained to protect the information.

(e) Major Command commanders, and Deputy Chiefs of Staff and comparable officials at Secretary of the Air Force and Headquarters United States Air Force offices implement this part.

(f) 11th Communications Squadron will provide Privacy Act training and submit Privacy Act reports for Headquarters United States Air Force and Secretary of the Air Force offices.

(g) Major Command Commanders: Appoint a command Privacy Act officer, and send the name, office symbol, phone number, and e-mail address to Air Force Chief Information Officer/P.

(h) Major Command and Headquarters Air Force Functional Chief Information Officers:

(1) Review and provide final approval on Privacy Impact Assessments (see Appendix E of this part).

(2) Send a copy of approved Privacy Impact Assessments to Air Force Chief Information Officer/P.

(i) Major Command Privacy Act Officers:

(1) Train base Privacy Act officers. May authorize appointment of unit Privacy Act monitors to assist with implementation of the program.

(2) Promote Privacy Act awareness throughout the organization.

(3) Review publications and forms for compliance with this part (do forms require a Privacy Act Statement; is Privacy Act Statement correct?).

(4) Submit reports as required.

(5) Review system notices to validate currency.

(6) Evaluate the health of the program at regular intervals using this part as guidance.

(7) Review and provide recommendations on completed Privacy Impact Assessments for information systems.

(8) Resolve complaints or allegations of Privacy Act violations.

(9) Review and process denial recommendations.

32 CFR Ch. VII (7-1-04 Edition)

(10) Provide guidance as needed to functionals on implementing the Privacy Act.

(j) Base Privacy Act Officers:

(1) Provide guidance and training to base personnel.

(2) Submit reports as required.

(3) Review publications and forms for compliance with this part.

(4) Review system notices to validate currency.

(5) Direct investigations of complaints/violations.

(6) Evaluate the health of the program at regular intervals using this part as guidance.

(k) System Managers:

(1) Manage and safeguard the system.

(2) Train users on Privacy Act requirements.

(3) Protect records from unauthorized disclosure, alteration, or destruction.

(4) Prepare system notices and reports.

(5) Answer Privacy Act requests.

(6) Records of disclosures.

(7) Validate system notices annually.

(8) Investigate Privacy Act complaints.

(l) System owners and developers:

(1) Decide the need for, and content of systems.

(2) Evaluate Privacy Act requirements of information systems in early stages of development.

(3) Complete a Privacy Impact Assessment and submit to the Privacy Act Officer.

Subpart B—Obtaining Law Enforcement Records and Confidentiality Promises

§ 806b.8 Obtaining law enforcement records.

The Commander, Air Force Office of Special Investigation; the Commander, Air Force Security Forces Center; Major Command, Field Operating Agency, and base chiefs of security forces; Air Force Office of Special Investigations detachment commanders; and designees of those offices may ask another agency for records for law enforcement under 5 U.S.C. 552a(b)(7). The requesting office must indicate in writing the specific part of the record desired and identify the law enforcement activity asking for the record.